Bitcoin: censorship-resistant currency and domain name system to the people

Dušan Barok
Networked Media
Piet Zwart Institute
Rotterdam, The Netherlands

July 20, 2011

Abstract

Bitcoin, the first decentralised currency was launched in 2009. Adopters use free software distributed in peer-to-peer computer network. The infrastructure provides a unique framework which allows pseudonymous users to make financial transactions stored transparently in the public record. User accounts and transactions cannot be controlled by the third party since the network does not depend upon any money issuing and processing central authority. The convergence of anonymity, transparency and decentralisation has long attracted technological libertarians criticising state interventionism and censorship. Bitcoin created a stir among activists pursuing cryptography in service of empowering civil liberties. It was adopted as a censorship-resistant donation system by organisations including Electronic Frontier Foundation, Freenet, and WikiLeaks. The paper explores the chain of events leading to this situation and examines the libertarian assumptions behind emancipatory promise of the new technology.

Keywords: Bitcoin, Namecoin, Electronic Frontier Foundation, WikiLeaks, cypherpunks, free software, cryptography, censorship, free speech, anonymity, pseudonymity, transparency, decentralisation, peer-to-peer, economy, domain name system

In June 2011, Electronic Frontier Foundation (EFF) issued announcement explaining why they decided to stop accepting bitcoins and removed the donation option from their website. The main concern was that “creating a new currency system [..] raises untested legal concerns related to securities law, the Stamp Payments Act, tax evasion, consumer protection and money laundering, among others” (Cohn, 2011). The announcement was preceded by the email response to a Bitcoin user who demanded an explanation of the sudden removal of the Bitcoin donation option from their website a month earlier. They answered that “legal tender is the best way to help EFF support online civil liberties” (Radracer, 2011). Bitcoin, a novel censorship-resistant digital currency still in its infancy and surrounded by legal ambiguities, was a natural candidate to gain support of the organisation which fought for free speech and against internet censorship numerous times. Reality was that EFF found too risky to jump on a digital money wagon, and simply declined to take risk promoting the experimental project.

Although EFF did not explicitly exclude its possible legal assistance if Bitcoin needs it, it was a rather big disappointment for the Bitcoin community, especially because earlier EFF used several occasions to praise the project publicly. In an unlikely setting. At the peak of Cablegate case in early December 2010, WikiLeaks suffered from several attacks which revealed vulnerabilities of the whistleblowing project. EveryDNS stopped providing WikiLeaks its domain name server service, and Amazon dropped its webhosting services, forcing them to search for servers elsewhere. The arbitrary denials of service were followed by PayPal, Visa, Mastercard and Bank of America cutting off their financial services to WikiLeaks. The organisation fundamentally relying on hierarchical DNS system and centralised financial networks became a subject of politically motivated censorship in its business of distribution of information. Accompanied by media attacks from various sides of the political spectrum, the censoring pressure put in motion resentments of global audience which felt directly affected, and protest actions followed. EFF took part protesting against censorship of a free flow of information on the Internet. They used the opportunity to inform about several censorship-resistant software tools. Next to well-known Tor anonymiser and recently started Dot-P2P project for distributed DNS, they also endorsed software a very few heard about: Bitcoin, a decentralised digital currency (Palmer, 2010; Reitman, 2011).

At an enigmatic event in this context, at the WikiLeaks protest rally in San Francisco, EFF Activist Director Rainey Reitman gave a speech (CarolHarveySF, 2010) in which Bitcoin was mentioned probably for the first time in a public gathering. EFF viewed Bitcoin as a tool which has potential to bypass centralised financial services, and provide privacy and anonymity these institutions disrespect and misuse for political purposes. In addition, several months later the Bitcoin technology was also implemented to provide a domain system that bypasses the hierarchical DNS, offering itself as a strong infrastructural mechanism for free speech initiatives, to make them far less vulnerable to censorship. Distributed digital currency is an unlikely addition to toolset supporting freedom of speech civil libertarians and activists consider a fundamental right in free society.

Digital currencies were discussed on cryptography mailing lists already in the nineties. Cryptographers shown that credit cards are highly insecure, and also did not work for micropayments. Two alternative systems got higher visibility than the others: David Chaum's DigiCash (1993-1998) and Douglas Jackson and Barry K. Downey's E-gold (1996-2009). However, neither of them proved to be sustainable. Netherlands-based DigiCash failed mainly due to its CEO's unpredictable character making last-minute vetoes of deals with companies that would have made his currency a standard for electronic money: Microsoft, Netscape, Visa, ING, Goldman Sachs (Grigg, 1999). E-gold management on the other hand was found guilty of money laundering and operating an unlicensed money-transmitting business. Their major vulnerability occurred to be a structural reliance on a trusted third party, a corporate legal body issuing money and verifying transactions. The corporations were not resistant to legal or extralegal attacks from outside, and at the same time possessed power to induce censorship on their users, the customers.

The answer was to decentralise the authority: get rid of the trusted third party. The solution had to be twofold: it had to specify who and how issues money in the system, and at the same time develop a security mechanism to prevent fraud, ie. users from spending the same money twice.

Bitcoin is the first attempt in decentralising the money issuance by being developed on top of purely peer-to-peer network. That required a substantial novelty in software design to maintain such network secure. In a decentralised currency framework, the main challenge is to make participants sure that money they receive is genuine, even if they don't trust a sender. Nick Szabo (2011) noted that the implementation was far from obvious: "Bitcoin ideas [..] required a very substantial amount of unconventional thought, not just about the security technologies [..], but about how to choose and put together these protocols and why. Bitcoin is not a list of cryptographic features, it's a very complex system of interacting mathematics and protocols in pursuit of [..] a goal".

To achieve this, Bitcoin brings together several developments in cryptography. Most of them are mentioned in the paper published by anonymous entity Satoshi Nakamoto (2008): Hash tree (published in 1979), public keys (1980), cryptographic timestamps (1991), Hashcash proof-of-work system (1997), Byzantine-resilient peer-to-peer replication (1999), SHA-256 (2001).

The goal of the system is to provide a framework for secure transactions without reliance on financial institutions. The verification process involves digital signatures. When user performs a transaction, her Bitcoin software performs a mathematical operation to combine the other party's public key and her own private key with the amount of bitcoins that she wants to transfer. The result of that operation is then sent out across the distributed Bitcoin network so the transaction can be verified by Bitcoin software clients not involved in the transfer. Those clients make two checks on a transaction. One uses the public key to confirm that the true owner of the pair sent the money, by exploiting the mathematical relationship between a person's public and private keys; the second refers to a public transaction log stored on the computer of every Bitcoin user to confirm that the person has the bitcoins to spend. When a client verifies a transaction, it forwards the details to others in the network to check for themselves. In this way a transaction quickly reaches and is verified by every Bitcoin client that is online (Simonite, 2011).

But this solves only a part of the problem of a distributed currency. The network has to decentralise a money issuing role of financial institutions. In a solution to this problem, Bitcoin combines security of the network with the money issuance. Money is issued as a reward for contributing computational power to process and verify transactions within the network. On a technical level, it uses proof-of-work as the solution to Byzantine Generals' Problem (Nakamoto, 2008*c*).

Although the solution is very far from trivial, for many in the crypto community in last two decades there has been more fundamental question: why do we need a cryptocurrency? For Szabo (2011), "the 'why' was by far the biggest stumbling block – nearly everybody who heard the general idea thought it was a very bad idea." The Libtech mailing list he had operated discussed decentralised currency systems extensively. "Myself [Szabo authored Bit gold proposal for digital currency, 1998], Wei Dai [B-money proposal, 1998], and Hal Finney [designed RPOW token system built upon proof-of-work algorithm, 2004] were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai). Only Finney and Nakamoto were motivated enough to actually implement such a scheme. The 'why' requires coming to an accurate understanding of the nature of two difficult and almost always misunderstood topics, namely trust and the nature of money. The overlap between cryptographic experts and libertarians who might sympathize with such an idea is already rather small."

This overlap was foundational to the Cypherpunks mailing list, which discussed the technical and politico-economic context of cryptographic communication since the early nineties. The U.S. government had long prevented making cryptographic software publicly available and treated it as a threat to national security, particularly as a munition, and thus subject to arms trafficking export controls. In 1991 Phil Zimmermann developed Pretty Good Privacy (PGP) program and released it into free circulation, making it the first widely available program implementing public-key cryptography famously invented by Diffie and Hellman fifteen years earlier (1976). The consequent criminal investigation of Zimmermann by the government for "munitions export without a license" (distribution of PGP software outside US borders) gave the crypto community a strong impetus to organise regular meetings, start a mailing list, and develop and spread crypto software. The Cypherpunks list was started in 1992 and in its activity peak five years later it had more than a thousand subscribers. Among them many influential cryptographers and free software developers: Adam Back, the author of Hashcash proof-of-work system; Julian Assange, the founder of WikiLeaks; Bram Cohen, the creator of BitTorrent; John Young of Cryptome.org and WikiLeaks ex-member; Hal Finney, the author of reusable proof-of-work system, and others who were directly involved in development of PGP, anonymous remailers, SSL, Linux kernel, or Tahoe-LAFS decentralised filesystem. The cypherpunks shared a strong anti-authoritarian attitude and envisioned free software enabled home-brewed privacy structures that the government couldn't crack.

The combination of cryptography, free software entrepreneurship, and celebration of emancipatory potential of the Internet, with the hostile anti-governmental affect gave raise to a new political vision. All three Cypherpunks list founders were Californian free software entrepreneurs and outspoken civil libertarians of strong caliber. Tim May, a physicist who retired from Intel in the mid-eighties, envisaged the future as an Ayn Rand utopia of autonomous individuals dealing with each other as they pleased. As the author of *Crypto Anarchist Manifesto* (1992) he imagined utopia with digital money, anonymous networks, digital pseudonyms, black markets, and collapsed governments, where only elites with control over technology would prosper. Ultimate goal of mathematician Eric Hughes was combining pure-market capitalism and freedom fighting. In his world view, governments were a constant threat to the well-being of citizens, and individual privacy was a citadel constantly under attack by the state (Levy, 2001, p.258–259). The two were joined by John Gilmore, a former high rank employee of Sun Microsystems, who co-founded EFF two years earlier. In one of his court cases, he sued governmental agencies over releasing NSA cryptographic textbooks into the public domain, and won. Considering the legal system inefficient, Gilmore (1991) wished a "guarantee – with physics and mathematics, not with laws – that we can give ourselves real privacy of personal communications." Cypherpunks valued personal privacy above all other considerations, although not all of them openly subscribed to the anarcho-capitalist libertarianism of their founders (for example Zimmermann, Finney, or Assange were alien to it).

EFF was affiliated with cypherpunks through Gilmore. Being financially supported by Silicon Valley entrepreneurs the organisation defended cypherpunk ideals in court cases against the government numerous times. In a case brought in 1995, EFF represented Daniel J. Bernstein who wanted to publish a paper and associated source code on his Snuffle encryption system. After four years, court ruled that software source code was a speech protected by the First Amendment and that the government's regulations preventing its publication were unconstitutional. This changed the rules of the game. EFF defended software as a free speech right, disabling the government from censoring the software export. Software companies and cryptographers celebrated. EFF counted another victory after claiming "independence of cyberspace" in 1997 when in *Reno v. ACLU* decision U.S. Supreme Court recognized that free speech on the Internet merits the highest standards of Constitutional protection. EFF participated as both plaintiff and co-counsel in the case, which successfully challenged the online censorship provisions of the Communications Decency Act of 1996. Cypherpunks were free to pursue their ideals without interference from the government: software and the Internet were protected as a free speech under the US Constitution.

Although early messages from Nakamoto (2008*a*) suggest that Bitcoin's appeal to libertarians was largely a marketing manoeuver, it can be considered a brainchild of cypherpunk core values: importance of anonymity, independence from the central authority, and freedom through free software. Yet it is unclear whether Nakamoto was on the Cypherpunks list or familiar with it. He did not adhere to the ideology of free market anarchist society in any of his messages posted between November 2008 and December 2010 (Nakamoto, 2008*a*, 2009–2010*a*).

Nakamoto discussed technicalities of the Bitcoin paper on the Cryptography mailing list shortly before the first client was launched in January 2009. Early adopters installed the software and began hashing. The computer which found a solution was rewarded by fixed sum of bitcoins issued by the network. The community of 'miners' grew and began exchanging bitcoins for services and other goods, including fiat money, such as dollars or euro.

But is Bitcoin money? Szabo (2011) maintains that "there's nothing like Nakamoto's incentive-to-market scheme to change minds about [whether Bitcoin can work as money]. Thanks to RAMs full of coin with 'scheduled deflation', there are now no shortage of people willing to argue in its favor." This is one reason for a popular myth viewing Bitcoin as a pyramid game, a Ponzi scheme. But while the system strongly incentives users to promote it to the others and build an actual economy on it, there is no authority to guarantee any profits to investors (*Bitcoin wiki: Myths*, 2011). The community has been actively supporting civil liberties and free software organisations. EFF was the first well known organisation to offer bitcoin donations to. It took three months to collect the donations, write a letter, and communicate with EFF staff until the organisation finally included Bitcoin as a "help out" option on their website in November 2010 (Kiba, 2010*b*; ichi, 2010; foreverD, 2010).

Despite its incentive-to-market the community learnt to maintain the network sustainable in the first place. When WikiLeaks was discussed on Bitcoin forums as a donation candidate in December 2010, Nakamoto (2010*c*) made a public plea to Wikileaks not to accept bitcoin donations. One of Nakamoto's (2010*b*) last messages on Bitcoin forum was a comment to an article speculating whether Wikileaks will trigger raise of the new virtual currency: "It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us". The community indeed withdrawn from offering the donations, and admitted it was not mature for massive attention at that stage of development.

Independence from the central authority and any other third-party creates unique environment. All Bitcoin transactions including issuance of new money are based on cryptographic proof (proof-of-work) instead of trust. There is no accountable institution which can be targeted and shut down, the system is fully distributed in peer-to-peer network. In legacy of tools for decentralised peer-to-peer filesharing (Gnutella and its follow-ups), and anonymous online communication in decentralised infrastructure (Tor), Bitcoin goes a step further to provide a framework for decentralised economy.

Anonymity is not built in Bitcoin by default. To stay hidden, one has to generate a new address for each transaction, and use an anonymising service such as Tor. But regardless on that all transactions made within the system are public and fully traceable. Besides the development of the Bitcoin client and mining software, the community also builds services around the public record of transactions (Blockexplorer.com, Bitcoinmonitor.com, Bitcoincharts.com). Individual anonymity is an option (Nakamoto, 2008*b*), while the software and transaction data are in the public domain. Satoshi Nakamoto pseudonymously designed the open system (Bitcoin was published under open-source MIT license which is compatible with GPL), transparent economy of pseudonymous participants.

Development of Dot-P2P project for distributed domain name system independent from ICANN authority and any other ISP's DNS service was announced in November 2010 (Ernesto, 2010). The idea was to base it on BitTorrent technology, but the main problem was to find a solution on how to decentralise allocation of domain names. Similar discussions were held in parallel to launch of Bitcoin system, which was offering itself to provide a platform for such enterprise. The community began pledging for the idea (Kiba, 2010*a*), and finally in April 2011, the first version of Namecoin was released (Vinced, 2011). The software uses a new blockchain, separate from the main Bitcoin chain, and introduces a fully functional decentralised DNS system with two thousand *.bit* domains registered as of time of this writing (*Dot-BIT Namecoin Project Wiki: Main Page*, 2011). System design prevents any entity to take over a domain from its owner.

The combination of transparency, optional anonymity, and absence of the central authority makes Bitcoin and Namecoin a strong tool for people and organisations facing a danger of financial and domain censorship. By adopting the technology, they gain an uncensorable toolset: a donation channel, a financial account, and domains. Accepting donations doesn't require a bank account at a traditional financial institution and thus there is no legal entity needed to process them. Nor it is needed in order to own a Namecoin domain. In June, WikiLeaks (2011*a*,*b*) publicly endorsed Bitcoin and Namecoin and several days later included the bitcoin donation option on their website. They followed the example of free software initiatives such as Tahoe-LAFS, I2P, Freenet, Torservers.net, and Free Software Foundation.

When EFF withdrawn from accepting bitcoins because of the legal vulnerability stemming from cashing out their income for taxable fiat currencies, they missed to consider another novel feature of the system. Or rather its liberatory potential. The fact that in the meantime the peer-to-peer economy with marketplace has been growing outside of the fiat money system. Bitcoin marketplace offers increasing variety of goods and services.

Organisations can use bitcoins to compensate volunteers, contributors, software developers, or cover hosting and domain costs. They can opt to spend their donations where they're coming from, within the Bitcoin community.

All in all, Bitcoin and Namecoin are the latest additions to a field of cryptographic free software along with PGP/GPG, Freenet, Tor, I2P, and Tahoe-LAFS, enabling censorship-resistant internet access, communication, filesharing, domain system, and now currency and market. While not being completely bullet-proof, the software is backed up by the community developing new versions and more tools.

Designed to set-off legal precedents, the main challenge for Bitcoin is to move beyond its liberatory potential. As with the arrival of web and Californian Ideology two decades earlier (Barbrook & Cameron, 1994), the Bitcoin community is now haunted by the ideology of free society to be liberated by the adoption of new technologies and free market. This view was criticised for producing the gap between those who have access to technology, and "late adopters" – those who may "have [it] later" (Rossetto, 1995), who are excluded from participating on making the community.

In the promising start, Bitcoin community affiliated itself with initiatives which help people with limited Internet access to bypass censorship and enable free speech. But while it is necessary to provide excluded people with the access in order to link them to community, the access alone is not sufficient. If Bitcoin is to become tool for free society in democratic sense, it has to bring its *free* and *open* features to their full potential, and to be usable by the broad *public*.

References

Barbrook, R. & Cameron, A. (1994). 'The Californian Ideology'. [online] Available at http://www.imaginaryfutures.net/2007/04/17/the-californian-ideology-2/ [Accessed 30 June 2011].

Bitcoin wiki: Myths (2011). [online] Available at: http://en.bitcoin.it/wiki/Myths#It_s_a_giant_ponzi_scheme [Accessed 15 June 2011].

CarolHarveySF (2010). 'Pt 3 – In San Francisco, Rainey Reitman on Wikileaks, Manning, Assange'. [video online] (Published 18 December) Available at: http://www.youtube.com/watch?v=9Ti5O3TI3iw [Accessed 18 June 2010].

Cohn, C. (2011). 'EFF and Bitcoin'. [online] San Francisco: Electronic Frontier Foundation (Published 20 June) Available at: http://www.eff.org/deeplinks/2011/06/eff-and-bitcoin [Accessed 21 June 2011].

Diffie, W. & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Trans. on Info. Theory* **IT-22**, 644–654. [online] Available at: http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf [Accessed 11 July 2011].

Dot-BIT Namecoin Project Wiki: Main Page (2011). [online] Available at: http://dot-bit.org/Main_Page [Accessed 12 June 2011].

Ernesto (2010). BitTorrent Based DNS To Counter US Domain Seizures. *TorrentFreak*. [online] (Published 30 November) Available at: http://torrentfreak.com/bittorrent-based-dns-to-counter-us-domain-seizures-101130/ [Accessed 10 June 2011].

foreverD (2010). 'Re: Letter to the EFF'. *Bitcoin Forum* [online] (Published 9 November) Available at: http://forum.bitcoin.org/index.php?topic=804.msg20948#msg20948 [Accessed 10 June 2011].

Gilmore, J. (1991). 'Privacy, Technology, and the Open Society'. [online] Available at: http://www.toad.com/gnu/cfp.talk.txt [Accessed 15 June 2011].

Grigg, I. (1999). ‘How DigiCash Blew Everything’. *Philodox* mailing list. Translated from Dutch. [online] (Sent 10 February) Available at: http://www.xent.com/FoRK-archive/feb99/0077.html [Accessed 16 June 2011].

ichi (2010). ‘Re: Letter to the EFF’. *Bitcoin Forum* [online] (Published 25 August) Available at: http://forum.bitcoin.org/index.php?topic=804.msg11111#msg11111 [Accessed 10 June 2011].

Kiba (2010*a*). ‘BitDNS Bounty (3500 BTC)’. *Bitcoin Forum* [online] (Published 4 December) Available at: http://forum.bitcoin.org/?topic=2072.0 [Accessed 26 June 2011].

Kiba (2010*b*). ‘EFF Donations Thread’. *Bitcoin Forum* [online] (Published 10 August) Available at: http://forum.bitcoin.org/?topic=778.0 [Accessed 10 June 2011].

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. Viking. New York.

May, T. (1992). ‘The Crypto Anarchist Manifesto’. [online] Available at: http://www.activism.net/cypherpunk/crypto-anarchy.html [Accessed 20 May 2011].

Nakamoto, S. (2008*a*). ‘Bitcoin P2P e-cash paper’. *Cryptography* mailing list. [online] (Sent November) Available at: http://www.mail-archive.com/cryptography@metzdowd.com/msg10001.html [Accessed 17 June 2011].

Nakamoto, S. (2008*b*). ‘Bitcoin P2P e-cash paper’. *Cryptography* mailing list. [online] (Sent 1 November) Available at: http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html [Accessed 20 May 2011].

Nakamoto, S. (2008*c*). ‘Re: Bitcoin P2P e-cash paper’. *Cryptography* mailing list. [online] (Sent 13 November) Available at: http://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html [Accessed 20 May 2011].

Nakamoto, S. (2009–2010*a*). ‘Bitcoin Forum’. [online] Available at: http://forum.bitcoin.org/index.php?action=profile;u=3;sa=showPosts [Accessed 17 June 2011].

Nakamoto, S. (2010*b*). ‘Re: PC World Article on Bitcoin’. *Bitcoin Forum* [online] (Published 11 December) Available at: http://forum.bitcoin.org/index.php?topic=2216.msg29280#msg29280 [Accessed 10 June 2011].

Nakamoto, S. (2010*c*). ‘Re: Wikileaks contact info?’. *Bitcoin Forum* [online] (Published 5 December) Available at: http://forum.bitcoin.org/index.php?topic=1735.msg26999#msg26999 [Accessed 10 June 2011].

Palmer, C. (2010). ‘Constructive Direct Action Against Censorship’. [online] San Francisco: Electronic Frontier Foundation (Published 14 December) Available at: http://www.eff.org/deeplinks/2010/12/constructive-direct-action-against-censorship [Accessed 1 June 2011].

Radracer (2011). ‘Re: Letter to the EFF’. *Bitcoin Forum* [online] (Published 1 June) Available at: http://forum.bitcoin.org/index.php?topic=804.msg158197#msg158197 [Accessed 15 June 2011].

Reitman, R. (2011). ‘Bitcoin – A Step Toward Censorship-Resistant Digital Currency’. [online] San Francisco: Electronic Frontier Foundation (Published 20 January) Available at: http://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant [Accessed 15 June 2011].

Rossetto, L. (1995). ‘Response to The Californian Ideology’. [online] Available at: http://www.imaginaryfutures.net/2007/04/20/wired-editor-responds-to-the-californian-ideology/ [Accessed 30 June 2011].

Simonite, T. (2011). What Bitcoin Is, and Why It Matters. *Technology Review.* [online] (Published 25 May) Available at: http://www.technologyreview.com/computing/37619/ [Accessed 15 June 2011].

Szabo, N. (2011). Bitcoin, what took ye so long?. *Enumerated.* [blog] 28 May, Available at: http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html [Accessed 20 June 2011].

Vinced (2011). ‘[announce] Namecoin a distributed naming system based on Bitcoin’. *Bitcoin Forum* [online] (Published 18 April) Available at: http://forum.bitcoin.org/?topic=6017.0 [Accessed 11 June 2011].

WikiLeaks (2011*a*). ‘Namecoin and Bitcoin will be revolutionary http://is.gd/8zKOTT see “Orwell’s Dictum” http://is.gd/2hsOWh’. *Twitter* [online] (Published 9 June) Available at: http://twitter.com/#!/wikileaks/statuses/78906603948093440 [Accessed 10 June 2011].

WikiLeaks (2011*b*). ‘WikiLeaks now accepts anonymous Bitcoin donations on 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v’. *Twitter* [online] (Published 15 June) Available at: http://twitter.com/#!/wikileaks/statuses/80774521350668288 [Accessed 26 June 2011].

Bibliography

Cypherpunks mailing list archive. [online] 1992-1998, Available at: http://cryptome.org/cpunks/cpunks-92-98.zip

Levy, S., 2001. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age.* New York: Viking.

Levy, S., 1993. Crypto Rebels, *Wired* Issue 1.02, [online] Available at: http://www.wired.com/wired/archive/1.02/crypto.rebels.html

Manne, R., 2011. Julian Assange: The Cypherpunk Revolutionary. *The Monthly*, March 2011, [online] Available at:
http://www.themonthly.com.au/julian-assange-cypherpunk-revolutionary-robert-manne-3081

May, T., 1992. *The Crypto Anarchist Manifesto.* [online] Available at: http://www.activism.net/cypherpunk/crypto-anarchy.html

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [online] Available at: http://bitcoin.org/bitcoin.pdf